Journal of Pure and Applied Algebra 79 (1992) 1–13
North-Holland

A resultant criterion and formula for the inversion of a rational map in two variables

Kossivi Adjamagbo

Département de Mathématiques, Université de Paris VI, U.F.R. 20, S.D.I. 6183, 4, Place Jussieu, 75252 Paris Cédex 5, France

Pierre Boury

Ecole Nationale des Ponts et Chaussées, CERMA, B.P. 105, 93167 Noisy-Le-Grand, France

Communicated by M.F. Coste-Roy
Received 5 November 1990
Revised 1 August 1991

Abstract

Adjamagbo, K. and P. Boury, A resultant criterion and formula for the inversion of a rational map in two variables, Journal of Pure and Applied Algebra 79 (1992) 1–13

Generalizing the main theorem of Adjamagbo and van den Essen in their article "A resultant criterion and formula for the inversion of a polynomial map in two variables" (J. Pure Appl. Algebra 64 (1990) 1–6), we characterize in terms of resultant the birationality of a couple F of rational fractions in two variables over a field. From this characterization, we deduce first precise information about the degree of the couples of relatively prime polynomials which define the inverse of a birational F, then an inversion formula for a birational F, and finally two new algorithms for testing the birationality of F and computing its inverse when it exists.

1. Introduction

Given K a field, $K(X_1, X_2)$ the field of rational fractions in variables X_1 and X_2 over K, and $F = (F_1, F_2) \in K(X_1, X_2)^2$, let us consider the following natural problems:

(1) How to know whether F is birational or not, i.e. whether the subfield $K(F_1, F_2)$ of $K(X_1, X_2)$ generated by F_1 and F_2 is equal to $K(X_1, X_2)$ or not.

(2) Knowing that F is birational, how to compute $G = (G_1, G_2) \in K(X_1, X_2)^2$ such that $G_i(F_1, F_2) = X_i$ for $1 \leq i \leq 2$.

Recently, Shannon and Sweedler [8] (see also [6]), solved these problems (and more generally for any number of indeterminates) in terms of the Groebner basis

of an ideal associated to F, generalizing previous results and methods of van den Essen [9], and Shannon and Sweedler [7] concerning polynomials.

But, using Groebner bases, being in practice more heavily than computing resultants of two polynomials in one variable (even for the best computer algebra systems), solving problems (1) and (2) in terms of resultants as done in [5] and [1] for the polynomial case, remained to be expected.

Furthermore, it seems difficult to get any information about birational maps in two variables from their characterization in terms of Groebner bases.

The main result of this paper, the resultant criterion theorem (Theorem 3.6) brings this expected solution to problem (1) and (2). It asserts that, Y_1 and Y_2 being new variables and P_i and Q_i relatively prime polynomials in X_1 and X_2 over K such that $F_i = P_i/Q_i$ for $1 \leq i \leq 2$, F is birational if and only if, for each variable X_i, the resultant, with respect to the other variable, of $P_1 - Y_1Q_1$ and $P_2 - Y_2Q_2$ is defined and has the form $\lambda_i(S_iX_i - R_i)$, where λ_i is a nonzero polynomial in X_i, in which case

$$(R_1(X_1, X_2)/S_1(X_1, X_2), R_2(X_1, X_2)/S_2(X_1, X_2))$$

is the inverse of F.

Thanks to the well-known fecundity of the resultant properties, we deduce from the resultant criterion theorem very precise and unknown information about total and partial degrees of pairs of relatively prime polynomials which define a birational map and its inverse (Corollaries 4.2, 4.3 and 4.4). The most 'symmetric' (with respect to the birational map and its inverse) of these degrees formula (partial degree formula, Corollary 4.2) asserts that, for a birational $(F_1, F_2) \in K(X_1, X_2)^2$ with inverse $(G_1, G_2) \in K(X_1, X_2)^2$, P_i and Q_i (resp. R_i and S_i) relatively prime nonzero polynomials in X_1, X_2 over K such that $F_i = P_i/Q_i$ (resp. $G_i = R_i/S_i$) for $1 \leq i \leq 2$, and $(i, j, k, l) \in \{1, 2\}^4$ such that $i \neq j$ and $k \neq l$, we have:

$$\max(\deg_{X_k} R_i, \deg_{X_k} S_i) = \max(\deg_{X_j} P_l, \deg_{X_j} Q_l)\,.$$

From the resultant criterion theorem, we also deduce an inversion formula for a birational map in two variables (Corollary 4.8) which asserts that, with previous notations, for each variable Y_i, $1 \leq i \leq 2$, if A_i denotes a prime factor in $K[X_1, X_2, Y_i]$ of the resultant, with respect to the other variable Y_j, of $P_1(Y_1, Y_2) - X_1Q_1(Y_1, Y_2)$ and $P_2(Y_1, Y_2) - X_1Q_2(Y_1, Y_2)$ such that $A_i \notin K[Y_i]$, then

$$G_i = -A_i(X_1, X_2, 0)(\partial A_i/\partial Y_i)^{-1}\,.$$

At the end, we describe precisely two new algorithms (proofs of Corollaries 4.9

and 4.10), deduced from the resultant criterion, for solving our initial problems (1) and (2) with the help of an elementary computer algebra system, knowing how to compute, apart from the resultant of two polynomials in one variable, the greatest common factor of polynomials in one variable over a field or the unique factorization of polynomials in three variables over a field.

The proof of the resultant criterion theorem is based on properties of the resultant of two polynomials in one variable over a field and elements of algebraic geometry coming from commutative algebra like a refined Hilbert Nullstellensatz theorem (Lemma 3.7) or the dimension formula for a domain which is a finitely generated algebra over a field.

2. On the resultant of two polynomials in one variable

For completeness, let us recall some useful generalities about the resultants of two polynomials in one variable.

2.1. Recall. Let $(m, n) \in \mathbb{N}^2 - \{(0,0)\}$.

(1) If $mn > 0$, the Sylvester polynomial $S_{m,n}$ of type (m, n) in variables $U_0, \ldots, U_m$ and $V_0, \ldots, V_n$ is the following polynomial $S_{m,n}$ of $\mathbb{Z}[U_0, \ldots, U_m, V_0, \ldots, V_n]$:

$$S_{m,n} := \det \underbrace{\begin{bmatrix} U_m & \cdots & \cdots & \cdots & U_0 & & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ & & U_m & \cdots & \cdots & \cdots & U_0 \\ V_n & \cdots & \cdots & V_0 & & & \\ & \cdots & \cdots & \cdots & \cdots & & \\ & & \cdots & \cdots & \cdots & \cdots & \\ & & & V_n & \cdots & \cdots & V_0 \end{bmatrix}}_{n+m \text{ columns}} \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \end{matrix}\right\} \begin{matrix} n \text{ rows} \\ \\ \\ \\ \\ m \text{ rows} \\ \\ \end{matrix}$$

If $m = 0$, the Sylvester polynomial of type $(0, n)$ in variable U_0 is the polynomial $S_{0,n} := U_0^n$ of $\mathbb{Z}[U_0]$.

If $n = 0$, the Sylvester polynomial of type $(m, 0)$ in variable V_0 is the polynomial $S_{m,0} := V_0^m$ of $\mathbb{Z}[V_0]$.

If $A[T]$ is the ring of polynomials of one variable over a commutative ring A, $f = \sum_{0<k\leq m} u_k T^k$ and $g = \sum_{0<k\leq n} v_k T^k$ two elements of $A[T]$ such that $\deg_T f \leq m$ and $\deg_T g \leq n$, the resultant of type (m, n) of f and g with respect to T is the following element of A:

$$\mathrm{Res}_{m,n,T}(f, g) := \begin{cases} S_{m,n}(u_0, \ldots, u_m, v_0, \ldots, v_n) & \text{if } mn > 0\,, \\ S_{0,n}(u_0) & \text{if } m = 0\,, \\ S_{m,0}(v_0) & \text{if } n = 0\,. \end{cases}$$

Furthermore, if $u_m \neq 0$ and $v_n \neq 0$, then the resultant of f and g with respect to T is

$$\mathrm{Res}_T(f, g) := \mathrm{Res}_{m,n,T}(f, g) .$$

(2) The Sylvester polynomial $S_{m,n}$ is homogeneous of degree n (resp. m) in the variables $U_0, \ldots, U_m$ (resp. $V_0, \ldots, V_n$).

(3) $\deg_{U_0}(S_{m,n} - (-1)^{mn} U_0^n V_n^m) < n$ and $\deg_{V_0}(S_{m,n} - U_m^n V_0^m) < m$.

(4) Alternative property: if A is a domain, then $\mathrm{Res}_{m,n,T}(f, g) = 0$ if and only if $u_m = v_n = 0$ or f and g have a common root in an extension of A.

(5) If A is a domain with quotient field B, and $(f, g) \in A[T]^2 - A^2$, $\mathrm{Res}_T(f, g) = 0$ if and only if the G.C.F. of f and g in $B[T]$ is not an element of B.

(6) If A is a commutative ring and $(f, g) \in A[T]^2 - A^2$, then $\mathrm{Res}_T(f, g) = fu + gv$ for some $(u, v) \in A[T]^2$.

2.2. Lemma. *(m, n) and $A[T]$ being defined as previously, let Y_1 and Y_2 be two new variables, $(a, b, c, d) \in A[T]^4$ such that*

$$\max(\deg_T a, \deg_T b) \leq m , \qquad \max(\deg_T c, \deg_T d) \leq n ,$$

and

$$R := \mathrm{Res}_{m,n,T}(a - Y_1 b, c - Y_2 d) \in A[Y_1, Y_2] .$$

Then R has the following properties:

(1) $\deg_{Y_1} R \leq n$ *and* $\deg_{Y_2} R \leq m$.

(2) *If $b = d = 1$, $a = \sum_{0 \leq k \leq m} a_k T^k$ and $c = \sum_{0 \leq k \leq n} c_k T^k$, then*

$$\deg_{Y_1}(R - (-1)^{n+mn} c_n^m Y_1^n) < n ,$$

$$\deg_{Y_2}(R - (-1)^m a_m^n Y_2^m) < m .$$

Proof. (1) follows from 2.1(2) and (2) from 2.1(3). □

2.3. Lemma. *For P and Q two relatively prime polynomials in variables X_1 and X_2 over K, and $i \in \{1, 2\}$ such that* $\max(\deg_{X_i} P, \deg_{X_i} Q) > 0$, *we have*

$$\mathrm{Res}_{X_i}(P, Q) \neq 0 .$$

Proof. Let $j \in \{1, 2\}$ such that $i \neq j$. According to assumptions on P and Q, the G.C.F. of P and Q in $K(X_j)[X_i]$ belongs to $K(X_j) - \{0\}$. Then, the conclusion follows from 2.1(5). □

3. The resultant criterion theorem

3.1. Notations. As we already mentioned in the Introduction, throughout the whole paper, K will denote a commutative field, X_1, X_2 variables, $K(X_1, X_2)$ the field of rational fractions in X_1 and X_2 over K, $K[X_1, X_2]$ the ring of polynomials in X_1 and X_2 over K. We will also denote by $\bar{K}$ (resp. $\overline{K(X_1, X_2)}$) an algebraic closure of K (resp. $K(X_1, X_2)$), and for $(a, b) \in \overline{K(X_1, X_2)}^2$, by $K(a)$ (resp. $K(a, b)$) the subfield of $\overline{K(X_1, X_2)}$ generated by K and $\{a\}$ (resp. $\{a, b\}$). Y_1, Y_2 will denote two other variables.

3.2. Proposition. *For $F = (F_1, F_2) \in K(X_1, X_2)^2$ and $G = (G_1, G_2) \in \overline{K(X_1, X_2)}^2$ such that $H_1 = F_1(G_1, G_2)$ and $H_2 = F_2(G_1, G_2)$ are defined, the following propositions are equivalent:*

(i) *F_1 and F_2 are algebraically independent over K, and G_1 and G_2 are algebraically independent over K.*

(ii) *$F_1(G_1, G_2)$ and $F_2(G_1, G_2)$ are algebraically independent over K.*

Proof. Let us assume (i). So, F and G define K-endomorphisms φ_F and φ_G of $\overline{K(X_1, X_2)}$ such that $\varphi_F(X_i) = F_i$ and $\varphi_G(X_i) = G_i$ for $1 \leq i \leq 2$. Let φ_H be the homomorphism of $K[X_1, X_2]$ into $\overline{K(X_1, X_2)}$ such that $\varphi_H(p) = p(H_1, H_2)$ for $p \in K[X_1, X_2]$. Since φ_H is the restriction of $\varphi_G \circ \varphi_F$ to $K[X_1, X_2]$, it follows from the injectivity of φ_F and φ_G that φ_H is injective, which means (ii).

Let us now assume (ii) and let φ_G be the homomorphism of $K[X_1, X_2]$ into $\overline{K(X_1, X_2)}$ such that $\varphi_G(p) = p(G_1, G_2)$ for $p \in K[X_1, X_2]$, I the kernel of φ_G, and Q quotient field of the image of φ_G. Since the transcendence degree of $K(H_1, H_2)$ over K is 2 and $K(H_1, H_2) \subset K(G_1, G_2)$, the transcendence degree over K of $K(G_1, G_2)$, therefore of Q, is also 2. So the Krull dimension of $K[X_1, X_2]/I$ is 2, which means that $I = \{0\}$ (since the Krull dimension of $K[X_1, X_2]$ is also 2) and proves that G_1 and G_2 are algebraically independent over K. Let us denote by $\overline{\varphi_G}$ the extension of φ_G on $\overline{K(X_1, X_2)}$, by φ_H the K-endomorphism of $\overline{K(X_1, X_2)}$ such that $\varphi_H(X_i) = H_i$ for $1 \leq i \leq 2$, and by φ_F the homomorphism of $K[X_1, X_2]$ into $K(X_1, X_2)$ such that $\varphi_F(p) = p(F_1, F_2)$ for $p \in K[X_1, X_2]$. Since $\overline{\varphi_G} \circ \varphi_F$, which is the restriction of φ_H to $K[X_1, X_2]$, is injective, so is φ_F, which proves (i). □

3.3. Corollary. *For $F = (F_1, F_2) \in K(X_1, X_2)^2$, the number of $G = (G_1, G_2) \in K(X_1, X_2)^2$ such that $F_i(G_1, G_2) = X_i$ for $1 \leq i \leq 2$ is at most* 1.

Proof. Let $G = (G_1, G_2)$ be as in the corollary. According to Proposition 3.2, F and G define injective K-endomorphisms φ_F and φ_G of $K(X_1, X_2)$ such that $\varphi_F(X_i) = F_i$, $\varphi_G(X_i) = G_i$ and $\varphi_G \circ \varphi_F(X_i) = X_i$ for $1 \leq i \leq 2$. So φ_G is surjective, therefore bijective with inverse φ_F. Since φ_G is the inverse of φ_F, G is unique. □

3.4. Corollary. *For* $(F_1, F_2, G_1, G_2) \in K(X_1, X_2)^4$, *the following propositions are equivalent*:

(i) $G_i(F_1, F_2) = X_i$ *for* $1 \leq i \leq 2$.

(ii) $F_i(G_1, G_2) = X_i$ *for* $1 \leq i \leq 2$.

Proof. It is sufficient to prove that (i) $\Rightarrow$ (ii).

So, let us assume (i). According to Proposition 3.2, $F = (F_1, F_2)$ and $G = (G_1, G_2)$ define injective K-endomorphisms φ_F and φ_G of $K(X_1, X_2)$ such that $\varphi_F(X_i) = F_i$, $\varphi_G(X_i) = G_i$ and $\varphi_F \circ \varphi_G(X_i) = X_i$ for $1 \leq i \leq 2$. Since φ_F is surjective, it is bijective with inverse φ_G. So $\varphi_G \circ \varphi_F(X_i) = X_i$ for $1 \leq i \leq 2$, which means (ii). □

3.5. Definition. For $F = (F_1, F_2) \in K(X_1, X_2)^2$, F is said to be *birational* if it satisfies one of the following equivalent conditions:

(i) $K(F_1, F_2) = K(X_1, X_2)$.

(ii) $\exists (G_1, G_2) \in K(X_1, X_2)^2$ such that $G_i(F_1, F_2) = X_i$ for $1 \leq i \leq 2$.

(iii) $\exists (G_1, G_2) \in K(X_1, X_2)^2$ such that $F_i(G_1, G_2) = X_i$ for $1 \leq i \leq 2$.

If F is birational, the unique $G = (G_1, G_2) \in K(X_1, X_2)$ such that $G_i(F_1, F_2) = X_i$ for $1 \leq i \leq 2$ is called the *inverse* of F.

3.6. Theorem. (The resultant criterion of birationality in two variables.) *For* $F = (F_1, F_2) \in K(X_1, X_2)^2$, P_i *and* Q_i *relatively prime elements of* $K[X_1, X_2]$ *such that* $Q_1 Q_2 \neq 0$ *and* $F_i = P_i / Q_i$ *for* $1 \leq i \leq 2$, *the following two conditions are equivalent*:

(i) F *is birational*.

(ii) *For* $1 \leq i \leq 2$, *there exist relatively prime nonzero elements* R_i *and* S_i *in* $K[Y_1, Y_2]$, $(R_i, S_i) \notin K^2$ *and* $\lambda_i \in K[X_i] - \{0\}$ *such that*:

(1) $F \notin K(X_i)^2$,

(2) $\mathrm{Res}_{X_j}(P_1 - Y_1 Q_1, P_2 - Y_2 Q_2) = \lambda_i (S_i X_i - R_i)$ *for* $j \in \{1, 2\} - \{i\}$.

Furthermore, if F *satisfies* (ii), *then*:

(iii) $(R_1(X_1, X_2)/S_1(X_1, X_2), R_2(X_1, X_2)/S_2(X_1, X_2))$ *is its inverse*.

(iv) λ_i *is a greatest common factor of coefficients of* $\mathrm{Res}_{X_j}(P_1 - Y_1 Q_1, P_2 - Y_2 Q_2)$ *considered as a polynomial in* Y_1 *and* Y_2 *over* $K[X_i]$.

(v) *Every prime factor of* $\mathrm{Res}_{X_j}(P_1 - Y_1 Q_1, P_2 - Y_2 Q_2)$ *in* $K[X_i, Y_1, Y_2]$ *which does not belong to* $K[X_i]$ *is associated to* $S_i X_i - R_i$.

Proof. For $(i, j) \in \{1, 2\}^2$ such that $i \neq j$, let $m_i = \deg_{X_j}(P_1 - Y_1 Q_1)$, $n_i = \deg_{X_j}(P_2 - Y_2 Q_2)$, $a_{i,k}$ and $b_{i,k}$ elements of $K[X_i]$ such that $a_{i,k} - Y_k b_{i,k}$ is the leading coefficient of $P_k - Y_k Q_k$ with respect to X_j for $1 \leq k \leq 2$.

Let us first assume (i) and let $G = (G_1, G_2) \in K(X_1, X_2)^2$ be the inverse of F, R_1 and S_1 (resp. R_2 and S_2) relatively prime nonzero elements of $K[X_1, X_2]$ such that $G_i = R_i / S_i$ for $1 \leq i \leq 2$, $l_k \in \mathbb{N}$ and $\tilde{Q}_k \in K[X_1, X_2]$ such that $(S_1 S_2)^{l_k} Q_k(R_1/$

$S_1, R_2/S_2) = \tilde{Q}_k$ for $1 \le k \le 2$. (In fact, we may take $l_1 = \max(m_1, m_2)$ and $l_2 = \max(n_1, n_2)$.)

Let us assume the opposite of (1). Then $K(F_1, F_2) \subset K(X_i)$, hence $K(F_1, F_2) \neq K(X_1, X_2)$, which is inconsistent with (i). So we have (1), thus $L_i = \mathrm{Res}_{X_j}(P_1 - Y_1 Q_1, P_2 - Y_2 Q_2) \in K[X_i, Y_1, Y_2]$ is defined, and also $a_i = \mathrm{Res}_{X_j}(P_k, Q_k)$ for some $k \in \{1, 2\}$.

Since $\bar{K}$ is finite, a_i is nonzero by Lemma 2.3, $S_i(Y_1, Y_2)X_i - R_i(Y_1, Y_2)$ is nonzero by the relative primeness of S_i and R_i, $a_{i,1}(X_i) - Y_1 b_{i,1}(X)$ is nonzero by definition, it follows that

$$S = \{(x_i, y_1, y_2) \in \bar{K}^3 \mid a_i(x_i) \neq 0, S_i(y_1, y_2)x_i - R_i(y_1, y_2) \neq 0, \\ a_{i,1}(x_i) - y_1 b_{i,1}(x_i) \neq 0\}$$

is not empty. Therefore, according to the alternative property (2.1(4)), $L_i(x_i, y_1, y_2) \neq 0$ for $(x_i, y_1, y_2) \in S$, which proves that $L_i \neq 0$.

Now, for any $(x_i, y_1, y_2) \in \bar{K}^3$ such that $(S_1 S_2 \tilde{Q}_1 \tilde{Q}_2)(y_1, y_2) \neq 0$ and $S_i(y_1, y_2)x_i - R_i(y_1, y_2) = 0$, define $x_j = R_j(y_1, y_2)/S_j(y_1, y_2)$; we have

$$P_k(x_1, x_2) - y_k Q_k(x_1, x_2) = Q_k(x_1, x_2)(F_k(x_1, x_2) - y_k) = 0$$

for $1 \le k \le 2$, and then $L_i(x_i, y_1, y_2) = 0$ by the alternative property (2.1(4)).

Since $S_i(Y_1, Y_2)X_i - R_i(Y_1, Y_2)$ and

$$S_1(Y_1, Y_2)S_2(Y_1, Y_2)\tilde{Q}_1(Y_1, Y_2)\tilde{Q}_2(Y_1, Y_2)$$

are relatively prime and $S_i(Y_1, Y_2)X_i - R_i(Y_1, Y_2)$ is irreducible in $K[X_i, Y_1, Y_2]$, it follows from the refined Nullstellensatz (Lemma 3.7) that there exists $\lambda_i \in K[X_i, Y_1, Y_2] - \{0\}$ such that

$$(*) \qquad L_i = \lambda_i(S_i(Y_1, Y_2)X_i - R_i(Y_1, Y_2)) .$$

Let now $(k, l) \in \{1, 2\}^2$ such that $k \neq l$.

From (*) we have

$$\max(\deg_{X_k} S_i, \deg_{X_k} R_i) + \deg_{Y_k}(\lambda_i) = \deg_{Y_k}(L_i)$$

for all $\{i, k\} \in \{1, 2\}^2$. From Lemma 2.2(1), we have

$$\deg_{Y_k}(L_i) \le \max(\deg_{X_j} P_l, \deg_{X_j} Q_l) .$$

Hence

$$\max(\deg_{X_k} S_i, \deg_{X_k} R_i) \le \max(\deg_{X_j} P_l \deg_{X_j} Q_l) .$$

By the symmetry of F and G the last inequality is an equality. From this last equality it follows that $\deg_{Y_k}(\lambda_i) = 0$, so that $\lambda_i \in K[X_i] - \{0\}$, which proves (ii).

Let us now assume (ii) and let $(i, j) \in \{1, 2\}^2$ such that $i \neq j$. As a first step we will show that

$$a_{i,k}(R_i S_i^{-1}) - Y_k b_{i,k}(R_i S_i^{-1}) \neq 0 \quad \text{for some } k \in \{1, 2\} ,$$

viewed as a rational function in Y_1, Y_2. Let us assume otherwise.

So for any $(x_i, y_1, y_2) \in \bar{K}^3$ such that $S_i(y_1, y_2)x_i - R_i(y_1, y_2) = 0$ and $S_i(y_1, y_2) \neq 0$, we have $a_{i,k}(x_i) - y_k b_{i,k}(x_i) = 0$ for $1 \leq k \leq 2$. Since $S_i X_i - R_i$ is irreducible in $K[X_i, Y_1, Y_2]$, $S_i X_i - R_i$ and S_i are relatively prime in $K[X_i, Y_1, Y_2]$, it follows from the refined Nullstellensatz (Lemma 3.7) that there exists $a_k \in K[X_i, Y_1, Y_2]$ such that

$$a_{i,k} - Y_k b_{i,k} = a_k(S_i X_i - R_i) \quad \text{for } 1 \leq k \leq 2 .$$

These relations imply that $(R_i, S_i) \in K^2$, which is inconsistent with the hypothesis.

So $a_{i,k}(R_i S_i^{-1}) - Y_k b_{i,k}(R_i S_i^{-1}) \neq 0$ for at least one $k \in \{1, 2\}$.

Since

$$\begin{aligned} &\operatorname{Res}_{m_i, n_i, X_j}((P_1 - Y_1 Q_1)|_{X_i = R_i S_i^{-1}}, (P_2 - Y_2 Q_2)|_{X_i = R_i S_i^{-1}}) \\ &\quad = \operatorname{Res}_{X_j}(P_1 - Y_1 Q_1, P_2 - Y_2 Q_2)|_{X_i = R_i S_i^{-1}} \\ &\quad = \lambda_i(R_i S_i^{-1})(S_i R_i S_i^{-1} - R_i) = 0 , \end{aligned}$$

it follows from the alternative property (2.1(4)) that there exists $(g_{i,1}, g_{i,2}) \in \overline{K(Y_1, Y_2)}^2$ such that $g_{i,i} = R_i S_i^{-1}$ and $P_k(g_{i,1}, g_{i,2}) - Y_k Q_k(g_{i,1}, g_{i,2}) = 0$ for $1 \leq k \leq 2$.

We will show that $Q_k(g_{i,1}, g_{i,2}) \neq 0$ for $1 \leq k \leq 2$. Let us assume otherwise, i.e. that $Q_k(g_{i,1}, g_{i,2}) = 0$ for some $k \in \{1, 2\}$. Then we also have $P_k(g_{i,1}, g_{i,2}) = 0$. According to Lemma 2.3, $g_{i,i}$ is a root of a nonzero polynomial of $K[X_i]$, such that $g_{i,i} = R_i S_i^{-1} \in \bar{K} \cap K(Y_1, Y_2) = K$, which is inconsistent with the hypothesis.

So $Q_k(g_{i,1}, g_{i,2}) \neq 0$ for $1 \leq k \leq 2$. Therefore, $F_k(g_{i,1}, g_{i,2}) = Y_k$ for $1 \leq k \leq 2$.

According to Proposition 3.2, $g_{i,1}$ and $g_{i,2}$ are therefore algebraically independent over K for $1 \leq i \leq 2$. On the other hand, according to the definition of $(g_{1,1}, g_{1,2})$ and relations (ii)(2) for $i = 2$, we have

$$\lambda_2(g_{1,2})(S_2 g_{1,2} - R_2) = 0 .$$

Since $\lambda_2 \neq 0$ and $g_{1,1}$ and $g_{1,2}$ are algebraically independent over K, $\lambda_2(g_{1,2}) \neq 0$, thus $S_2 g_{1,2} - R_2 = 0$, which means $g_{1,2} = R_2 S_2^{-1}$.

Summing up, $F_k(R_1S_1^{-1}, R_2S_2^{-1}) = Y_k$ for $1 \leq k \leq 2$, which proves (i) and (iii), and achieves the proof of the theorem, since (iv) and (v) are obvious. □

3.7. Lemma. (Refined Nullstellensatz for prime ideals.) *Let I be a prime ideal of the ring $K[X_1, \ldots, X_n]$ of polynomials in variables $X_1, \ldots, X_n$ over K, P and Q polynomials of $K[X_1, \ldots, X_n]$ such that $P \notin I$ and $Q(x) = 0$ for every zero x of I in $\bar{K}^n$ which is not a zero of P. Then $Q \in I$.*

Proof. Since $(PQ)(x) = 0$ for every zero of I in $\bar{K}^n$, it follows from the classical Nullstellensatz that $PQ \in I$. Since $P \notin I$, it follows that $Q \in I$. □

4. Consequences of the resultant criterion theorem

Let us keep the notations of 3.1.

4.1. Corollary (Adjamagbo and Van den Essen [1, Theorem 1.1]). (The resultant criterion for the inversion of a polynomial map in two variables.) *For $F = (F_1, F_2) \in K[X_1, X_2]^2$, the following propositions are equivalent:*

(i) *F is birational and its inverse is polynomial (i.e. $K[F_1, F_2] = K[X_1, X_2]$).*

(ii) *For every $i \in \{1, 2\}$, there exist G_i in $K[Y_1, Y_2]$ and λ_i in K^* such that*

(1) $F \notin K[X_i]^2$,

(2) $\mathrm{Res}_{X_j}(F_1 - Y_1, F_2 - Y_2) = \lambda_i(X_i - G_i)$ *for* $j \in \{1, 2\} - \{i\}$.

Furthermore, if F satisfies (ii), *then $(G_1(X_1, X_2), G_2(X_1, X_2))$ is its inverse.*

Proof. Let us assume (i). It follows from the resultant criterion theorem that we have (ii) with $\lambda_i \in K[X_i] - \{0\}$.

Then, it follows from relations (ii)(2) and 2.1(3) that:

(α) If $G_i \in K[Y_k]$ for some $(i, k) \in \{1, 2\}^2$, then for $j \in \{1, 2\}$ such that $i \neq j$, $\mathrm{Res}_{X_j}(F_1 - Y_1, F_2 - Y_2)$ has the form $\pm(F_k(X_j) - Y_k)^m$, where $m = \deg_{X_j} F_l$, and therefore that $\lambda_i \in K^*$ (considering the leading coefficient of G_i with respect to Y_k in the right-hand side of (2)).

(β) If $G_i \notin K[Y_1] \cup K[Y_2]$ for some $i \in \{1, 2\}$, the leading coefficient of G_i with respect to Y_k belongs to K^* for every $k \in \{1, 2\}$.

Since F has the same property (β) as its inverse, it follows from (2), 2.1(3), and (β) that, under the condition of (β), $\lambda_i \in K^*$, which achieves the proof of (ii), and also of the corollary, since the implication (ii) $\Rightarrow$ (i) is obvious according to the resultant criterion theorem. □

4.2. Corollary. (Partial degrees formula for a birational map in two variables.) *Let $F = (F_1, F_2)$ be a birational element of $K(X_1, X_2)^2$, $G = (G_1, G_2) \in K(X_1, X_2)^2$ its inverse, P_i and Q_i (resp. R_i and S_i) relatively prime nonzero elements of $K[X_1, X_2]$ such that $F_i = P_i/Q_i$ (resp. G_i/S_i) for $1 \leq i \leq 2$, and $(i, j, k, l) \in \{1, 2\}^4$*

such that $i \neq j$ and $k \neq l$. Then we have

$$\max(\deg_{X_k} R_i, \deg_{X_k} S_i) = \max(\deg_{X_j} P_l, \deg_{X_j} Q_l)\,. \tag{4.1}$$

Proof. It follows from formula (2) of the resultant criterion theorem and from relations 2.2(1) of the Recall 2.2 that we have the formula deduced from (4.1) by substituting $\leq$ to $=$. Applying twice this inequality proves (4.1). □

4.3. Corollary. (Total degrees formula for a birational map in two variables.) *With the same notations as in Corollary* 4.2, *we have*

$$\begin{aligned}&\max(\deg_{X_1,X_2} R_i, \deg_{X_1,X_2} S_i)\\ &\quad = \deg_{Y_1,Y_2} \operatorname{Res}_{X_j}(P_1 - Y_1 Q_1, P_2 - Y_2 Q_2)\,. \qquad \square\end{aligned} \tag{4.2}$$

4.4. Corollary. (Total degrees formula for a polynomial birational map in two variables.) *Let $F = (F_1, F_2)$ be a birational element of $K[X_1, X_2]^2$, $(G_1, G_2) \in K(X_1, X_2)^2$ its inverse, R_i and S_i relatively prime nonzero elements of $K[X_1, X_2]$ such that $G_i = R_i/S_i$ for $1 \leq i \leq 2$, and $\{i, j, k, l\} \in \{1, 2\}^4$ such that $i \neq j$ and $k \neq l$. Then, for $i \in \{1, 2\}$ we have*

$$\max(\deg_{X_1,X_2} R_i, \deg_{X_1,X_2} S_i) = \max_{1 \leq k \leq 2}(\max(\deg_{X_k} R_i, \deg_{X_k} S_i))\,. \tag{4.3}$$

Proof. Let $P_i = F_i$ and $Q_i = 1$ for $1 \leq i \leq 2$.

According to formula (4.2), for $(i, j) \in \{1, 2\}^2$ such that $i \neq j$, we have

$$\max(\deg_{X_1,X_2} R_i, \deg_{X_1,X_2} S_i) = \max_{1 \leq k \leq 2}(\max(\deg_{X_j} P_k, \deg_{X_j} Q_k))\,.$$

Now, according to formula (4.1), we have

$$\begin{aligned}&\max_{1 \leq k \leq 2}(\max(\deg_{X_j} P_k, \deg_{X_j} Q_k))\\ &\quad = \max(\max(\deg_{X_1} R_i, \deg_{X_1} S_i), \max(\deg_{X_2} R_i, \deg_{X_2} S_i))\,. \qquad \square\end{aligned}$$

4.5. Corollary. (Gabber's degrees inequality for a polynomial birational map in two variables [2, Theorem 1.5, Remark 1.3, Corollary 1.4 and Footnote 4].) *With the same notations as in Corollary* 4.4, *we have*

$$\max(\deg_{X_1,X_2} R_i, \deg_{X_1,X_2} S_i) \leq \max(\deg_{X_1,X_2} F_1, \deg_{X_1,X_2} F_2)\,. \tag{4.4}$$

Proof. (4.4) follows from (4.2) and 2.1(3) of Recall 2.2. □

4.6. Corollary. *Let $F = (F_1, F_2)$ be a birational element of $K(X_1, X_2)^2$ such that $F_1 \in K(X_i)$ for some $i \in \{1, 2\}$. Then F_1 is homographic in X_i, that is, there exists $(a, b, c, d) \in K^4$ such that $ad - bc \neq 0$ and $F_1 = (aX_i + b)/(cX_i + d)$.*

Proof. Let P_1 and Q_1 be relatively prime elements of $K[X_i]$ such that $F_1 = P_1/Q_1$.

It follows from resultant criterion theorem of degrees formula that there exists $m \in \mathbb{N}$, and $(\lambda, R, S) \in K[X_i] \times K[Y_1, Y_2]^2$ such that a and b are relatively prime and $(P_1 - Y_i Q_1)^m = \lambda(SX_i - R)$. $P_1 - Y_1 Q_1$ and $SX_i - R$ being irreductible elements of $K[X_i, Y_1, Y_2]$, it follows that $m = 1$, $\lambda \in K^*$, and $\max(\deg_{X_i} P_1, \deg_{X_i} Q_1) = 1$. So there exists $(a, b, c, d) \in K^4$ such that $P_1 = aX_i + b$, $Q_1 = cX_i + d$. It follows from condition (1) of the resultant criterion theorem that $ad - bc \neq 0$. □

4.7. Corollary. (Characterization of birational map in one variable, see [4, Theorem 8.36, p. 514].) *For a rational fraction F in one variable X over K, the following propositions are equivalent*:

(i) *F is birational (i.e. $F(G) = G(F) = X$ for some $G \in K[X]$).*

(ii) *F is homographic (i.e. $F = (aX + b)/(cX + d)$, with $(a, b, c, d) \in K^4$ and $ad - bc \neq 0$).* □

4.8. Corollary. (Inversion formula for birational maps in two variables.) *Let (F_1, F_2) be a birational element of $K(X_1, X_2)^2$, (G_1, G_2) its inverse, P_i and Q_i relatively prime elements of $K[X_1, X_2]$ such that $F_i = P_i/Q_i$ for $1 \leq i \leq 2$, $(i, j) \in \{1, 2\}^2$ such that $i \neq j$, and A_i a prime factor of*

$$\mathrm{Res}_{Y_j}(P_1(Y_1, Y_2) - X_1 Q_1(Y_1, Y_2), P_2(Y_1, Y_2) - X_2 Q_2(Y_1, Y_2))$$

in $K[X_1, X_2, Y_i]$ such that $A_i \notin K[Y_i]$. Then

$$G_i = -A_i(X_1, X_2, 0)(\partial A_i/\partial Y_i)^{-1}. \qquad \square \tag{4.5}$$

4.9. Corollary. (Resultant and unique factorization algorithm for testing the birationality of a rational map and computing its inverse.) *There is an algorithm using essentially the resultant of two polynomials in one variable and unique factorization of polynomials in three variables over K, which tests whether an element of $K(X_1, X_2)^2$ is birational and computes its inverse when it exists.*

Proof. The following algorithm proves the corollary:

Input: A list (P_1, Q_1, P_2, Q_2) of nonzero elements of $K[X_1, X_2]$.

Output: **if** $F = (P_1/Q_1, P_2/Q_2)$ is birational

then a list (R_1, S_1, R_2, S_2) of nonzero elements of $K[X_1, X_2]$ such that $(R_1/S_1, R_2/S_2)$ is the inverse of F

else the empty list

Step 1: Data preparation.

Using unique factorization function of elements of $K[X_1, X_2]$, modify (P_1, Q_1, P_2, Q_2) such that P_1 and Q_1 (resp. P_2 and Q_2) are relatively prime.

Step 2: Elimination of trivial cases.
if $\max_{1\le k\le 2}(\max(\deg_{X_j} P_k, \deg_{X_j} Q_k)) = 0$ for some $j \in \{1, 2\}$
then return the empty list
Step 3: Resultants computation.
Compute $B_1 := \mathrm{Res}_{X_2}(P_1 - Y_1 Q_1, P_2 - Y_2 Q_2)$ and $B_2 := \mathrm{Res}_{X_1}(P_1 - Y_1 Q_1, P_2 - Y_2 Q_2)$.
Step 4: Resultants factorization.
Factorize B_1 (resp. B_2) in $K[X_1, Y_1, Y_2]$ (resp. $K[X_2, Y_1, Y_2]$).
Step 5: Prime factors test.
if B_1 (resp. B_2) has more than one factor whose total degree in Y_1 and Y_2 is >0 or if the multiplicity of such a prime factor is >1, or if the degree of such a prime factor in X_1 (or X_2) is >1
then return the empty list
Step 6: Computation of the inverse.
For $1 \le i \le 2$, let A_i be the unique prime factor of B_i with positive total degree in Y_1 and Y_2, $R_i := -A_i(0, Y_1, Y_2)$, $S_i := \partial A_i / \partial X_i$.
if S_1 or S_2 is zero
then return the empty list
else return $(R_1(X_1, X_2), S_1(X_1, X_2), R_2(X_1, X_2), S_2(X_1, X_2))$ □

4.10. Corollary. (Resultant and greatest common factor algorithm for testing the birationality of a rational map and computing its inverse.) *There is an algorithm using essentially the resultant of two polynomials in one variable and the greatest common factor of polynomials in one variable over K, and which tests whether an element of* $K(X_1, X_2)^2$ *is birational and computes its inverse when it exists.*

Proof. The following algorithm proves the corollary:

Input: A list (P_1, Q_1, P_2, Q_2) of nonzero elements of $K[X_1, X_2]$ such that P_1 and Q_1 (resp. P_2 and Q_2) are relatively prime.
Output: **if** $F = (P_1/Q_1, P_2/Q_2)$ is birational
then a list (R_1, S_1, R_2, S_2) of nonzero elements of $K[X_1, X_2]$ such that $(R_1/S_1, R_2/S_2)$ is the inverse of F
else the empty list

Step 1: Elimination of trivial cases.
if $\max_{1\le k\le 2}(\max(\deg_{X_j} P_k, \deg_{X_j} Q_k)) = 0$ for some $j \in \{1, 2\}$
then return the empty set
Step 2: Resultant computation.
Compute $A_1 := \mathrm{Res}_{X_2}(P_1 - Y_1 Q_1, P_2 - Y_2 Q_2)$ and $A_2 := \mathrm{Res}_{X_1}(P_1 - Y_1 Q_1, P_2 - Y_2 Q_2)$.
Step 3: Greatest common factor computation.
For $1 \le i \le 2$, compute $\lambda_i :=$ the greatest common factor of the coefficients of A_i considered as polynomial in Y_1 and Y_2 over $K[X_i]$ and modify A_i by dividing each of its coefficients by λ_i.

Step 4: Computation of the inverse.
For $1 \leq i \leq 2$,
if $\deg_{X_i} A_i > 1$
then return the empty list
Compute $R_i := -A_i(0, Y_1, Y_2)$ and $S_i := \partial A_i / \partial X_i$.
if S_1 or S_2 is zero
then return the empty list
else return $(R_1(X_1, X_2)/S_1(X_1, X_2), R_2(X_1, X_2)/S_2(X_1, X_2))$ □

References

[1] K. Adjamagbo and Van den Essen, A resultant criterion and formula for the inversion of a birational map in two variables, J. Pure Appl. Algebra 64 (1990) 1–6.
[2] H. Bass, E.H. Connell and D. Wright, The Jacobian conjecture: reduction of degree, and formal expansion of the inverse, Bull. Amer. Math. Soc. 7 (1982) 287–330.
[3] R. Hartshorne, Algebraic Geometry (Springer, New York, 1977).
[4] N. Jacobson, Basic Algebra II (Freeman, San Francisco, CA, 1980).
[5] H. McKay and S. S.-S. Wang, An inversion formula for two polynomials in two variables, J. Pure Appl. Algebra 40 (1986) 245–257.
[6] F. Ollivier, Invertibility of rational mappings and structural identifiability in automatics, in: Proceedings of ISSAC'89, Portland, OR (ACM, New York, 1989) 43–53.
[7] D. Shannon and M. Sweedler, Using Groebner bases to determine algebra membership, split surjective algebra homomorphisms and determine birational equivalence, J. Symbolic Comput. 6 (1988) 2–3.
[8] D. Shannon and M. Sweedler, Using Groebner bases to determine algebra membership, 1988 (Preprint).
[9] A. Van den Essen, A criterion to decide if a polynomial map is invertible and to compute the inverse, Comm. Algebra 18 (10) (1990) 3183–3186.